Council of the
European Union

**Brussels, 17 December 2015**
**(OR. en)**

**15361/15**

**LIMITE**

**DATAPROTECT 240**
**JAI 1012**
**DAPIX 244**
**FREMP 305**
**COMIX 700**
**CODEC 1742**

**Interinstitutional File:**
**2012/0010 (COD)**

**NOTE**

| | |
|---|---|
| From: | Mr. Claude Moraes, Chairman of the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament |
| On: | 18 December 2015 |
| To: | Mr. Ambassador Christian Braun, Permanent Representative, Council of the European Union |
| No. prev. doc.: | 15174/15 |
| Subject: | Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data [First reading]<br>- Confirmation of the final compromise with a vue to agreement |

Delegations will find enclosed a letter of Mr. Claude Moraes, Chairman of the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament to Ambassador Christian Braun, Chairman of the Permanent Representatives Committee, concerning Council's position at first reading on above mentioned Proposal for a Directive.

Committee on Civil Liberties, Justice and Home Affairs
The Chairman

IPOL-COM-LIBE D (2015) 61780

Strasbourg, 17 December 2015

Mr. Christian BRAUN
Ambassador,
Permanent Representative of Luxembourg
Council of the European Union
Rue de la Loi 175
1048 Brussels

D 204661 17.12.2015

**Subject: Council's First Reading Position on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (2012/0010(COD))**

Dear Ambassador Braun,

Following the positive outcome of the confirmation vote on the Data Protection Directive that took place in the meeting of the Committee on Civil Liberties, Justice and Home Affairs of 17 December 2015, I would like to inform you that the LIBE Committee considered positively the acceptance of the text set out in the Annex which reflects the outcome of the negotiations between the three Institutions.

Thus, I would like to inform you that, if this text was to be transmitted formally to the European Parliament as the Council's First Reading Position for this legislative proposal, I will recommend to the Members of the Committee on Civil Liberties, Justice and Home Affairs and subsequently to the Plenary that the Council's First Reading Position be accepted without amendments in Parliament's second reading, subject to verification by the lawyer linguists of both Institutions and the alignment of the relevant definitions with those agreed in the General Data Protection Regulation.

I would like to thank you and the previous Council Presidencies for the close cooperation on this file.

Yours sincerely,

Claude Moraes

Claude MORAES

Annex: text agreed

**<u>Annex to the ANNEX</u>**

Proposal for a

**DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Data Protection Supervisor,[1]

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty of the Functioning of the European Union lay down that everyone has the right to the protection of personal data concerning him or her.

[1] OJ C 192, 30.6.2012, p.7.

(2) The principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. This should contribute to the accomplishment of an area of freedom, security and justice.

(3) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data collection and sharing has increased spectacularly. Technology allows to make use of personal data on an unprecedented scale in order to pursue activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(4) This requires facilitating the free flow of data between competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security within the Union and the transfer to third countries and international organisations, while ensuring a high level of protection of personal data. These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement.

(5) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[2] applies to all personal data processing activities in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Community law', such as activities in the areas of judicial co-operation in criminal matters and police co-operation.

[2] OJ L 281, 23.11.1995, p. 31.

(6) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters[3] applies in the areas of judicial co-operation in criminal matters and police co-operation. The scope of application of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States.

(7) Ensuring a consistent and high level of protection of the personal data of individuals and facilitating the exchange of personal data between competent authorities of Members States is crucial in order to ensure effective judicial co-operation in criminal matters and police cooperation. To that aim, the level of protection of the rights and freedoms of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, should be equivalent in all Member States. Effective protection of personal data throughout the Union requires strengthening the rights of data subjects and the obligations of those who process personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.

(8) Article 16(2) of the Treaty on the Functioning of the European Union mandates the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.

(9) On that basis, Regulation EU …../XXX of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) lays down general rules to protect individuals in relation to the processing of personal data and to ensure the free movement of personal data within the Union.

[3] OJ L 350, 30.12.2008, p. 60.

(10) In Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal matters and police co-operation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of such data in the fields of judicial co-operation in criminal matters and police co-operation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.

(11) Therefore a distinct Directive should meet the specific nature of these fields and lay down the rules relating to the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law enforcement authorities but also any other body or entity entrusted by national law to exercise public authority and public powers for the purposes of this Directive. However, where such a body or entity processes personal data for other purposes than for the purposes of this Directive, Regulation EU/XXX applies. Therefore Regulation EU/XXX applies in cases where a body or entity**,** collects personal data for other purposes and further processes those personal data for compliance with a legal obligation to which it is subject e.g. financial institutions retain for the purposes of investigation, detection or prosecution certain data which are processed by them, and provide those data only to the competent national authorities in specific cases and in accordance with national law. A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive, while the application of Regulation EU/XXX remains unaffected for processing activities of the processor outside the scope of this Directive.

(11a) The activities carried out by the police or other law enforcement authorities are mainly focused on the prevention, investigation, detection or prosecution of criminal offences including police activities without prior knowledge if an incident is a criminal offence or not. These can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. Those activities performed by the above-mentioned authorities also include maintaining law and order as a task conferred on the police or other law enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law, which may lead to a criminal offence. Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of Regulation EU/XXX.

(11aa) The concept of a criminal offence within the meaning of this Directive should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union.

(11b) Since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security, activities of agencies or units dealing with national security issues and processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union should not be considered as activities falling within the scope of this Directive.

(12) In order to ensure the same level of protection for individuals through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent authorities, the Directive should provide harmonised rules for the protection and the free movement of personal data processed for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. The approximation of Member States' laws should not result in any lessening of the data protection they afford but should, on the contrary, seek to ensure a high level of protection within the Union. Member States should not be precluded from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.

(13) This Directive is without prejudice to the principle of public access to official documents. Under Regulation EU/XXX personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data.

(14) The protection afforded by this Directive should concern natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.

(15) The protection of individuals should be technologically neutral and not depend on the technologies used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means, as well as to manual processing if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Directive.

(15a) Regulation (EC) No 45/2001[4] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal instruments applicable to such processing of personal data should be adapted to the principles and rules of Regulation EU/XXX.

(15b) This Directive does not preclude Member States from specifying processing operations and processing procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular as regards personal data contained in a judicial decision or in records in relation to criminal proceedings.

(16) The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the individual directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous information, that is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is no longer identifiable.

[4] OJ L 8, 12.1.2001, p. 1.

(16a) Public authorities to whom data are disclosed in compliance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities, responsible for the regulation and supervision of securities markets, may not be regarded as recipients if they receive data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of these data by those public authorities should be in compliance with the applicable data protection rules according to the purposes of the processing.

(16aa) Genetic data should be defined as personal data relating to the genetic characteristics of an individual which have been inherited or acquired which give unique information about the physiology or health of that individual, resulting in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained. Considering the complexity and sensitivity of genetic information, there is a great risk of misuse and/or re-use for various purposes by the controller. Any discrimination based on genetic features should in principle be prohibited.

(17) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject; including information about the individual collected in the course of the registration for and the provision of health care services to the individual as referred to in Directive 2011/24/EU; a number, a symbol or a particular assigned to an individual to uniquely identify the individual for health purposes; information derived from the testing or examination of a body part or bodily substance, including genetic data and biological samples; or any information on, for example, a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as, for example, from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

(17a) All Member States are affiliated to the International Criminal Police Organisation (Interpol). To fulfil its mission, Interpol receives, stores, and circulates data to assist competent authorities to prevent and combat international crime. Therefore, it is appropriate to strengthen cooperation between the European Union and Interpol by promoting an efficient exchange of personal data whilst ensuring the respect for fundamental rights and freedoms regarding the automatic processing of personal data. When personal data is transferred from the European Union to Interpol, and to countries which have delegated members to Interpol, this Directive should apply, in particular the provisions on international transfers. This Directive should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol[5] and Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).[6]

---

[5] OJ L 27, 29.1.2005, p. 61–62.

[6] OJ L 205, 7.8.2007, p. 63–84.

(18) Any processing of personal data must be lawful, fair and transparent in relation to the individuals concerned, and only processed for specific purposes laid down by law. This does not in itself prevent the law enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned. The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined by Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and Article 47 of the Charter of Fundamental Rights of the European Union. Individuals should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate and relevant for the purposes for which the data are processed; this requires, in particular, ensuring that the data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. Personal data should only be processed if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Member States should lay down appropriate safeguards for personal data stored for longer periods for archiving in the public interest, scientific, statistical or historical use.

(19) For the prevention, investigation and prosecution of criminal offences it is necessary for competent authorities to process personal data, collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context to develop an understanding of criminal activities and to make links between different offences detected.

(19a) In order to maintain security of the processing and to prevent processing in breach of this Directive, personal data should be processed in a manner that ensures an appropriate level of security and confidentiality, including preventing unauthorised access to or use of personal data and the equipment used for the processing, taking into account available state of the art and technology and the costs of implementation in relation to the risks and the nature of the personal data to be protected.

(20) (…)

(20a) Personal data should be collected for specified, explicit and legitimate purposes within the scope of this Directive and not be processed for purposes incompatible with the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. If personal data is processed by the same or another controller for a purpose within the scope of this Directive other than the one for which it has been collected, such processing is compatible under the conditions that this processing is authorised in accordance with applicable legal provisions and is necessary and proportionate to that other purpose.

(21) The principle of accuracy of data should be applied taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of individuals and are in some cases not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

(22) (…)

(23) It is inherent to the processing of personal data in the areas of judicial co-operation in criminal matters and police co-operation that personal data relating to different categories of data subjects are processed. Therefore a clear distinction should, where applicable and as far as possible, be made between personal data of different categories of data subjects such as suspects, persons convicted of a criminal offence, victims and third parties, such as witnesses, persons possessing relevant information or contacts and associates of suspects and convicted criminals. This should not prevent the application of the right of presumption of innocence as guaranteed by the Charter of Fundamental Rights of the European Union and by the European Convention on Human Rights, as interpreted by the case law of the Court of Justice of the European Union and the European Court of Human Rights respectively.

(24) The competent authorities should ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. In order to ensure both the protection of individuals and the accuracy, completeness or the extent to which the personal data are up to date and reliability of the personal data transmitted or made available the competent authorities should, as far as possible, add necessary information in all transmissions of personal data.

(24a) Wherever this Directive refers to Member State law, a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned, however, such Member State law, legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it as required by the case law of the Court of Justice of the European Union and the European Court on Human Rights. Member State law regulating the processing of personal data within the scope of this Directive should specify at least the objectives, the personal data to be processed, the purposes of the processing and procedures for preserving the integrity and confidentiality of personal data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.

(24b) The processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security should cover any operation or set of operations which are performed upon personal data or sets of personal data for those purposes, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction, erasure or destruction. In particular, the rules of this Directive should apply to the transmission of personal data for the purposes of this Directive to a recipient not subject to this Directive. Such recipient should mean a natural or legal person, public authority, agency or any other body, to which the data are lawfully disclosed by the competent authority. Where data were initially collected by a competent authority for one of the purposes of this Directive, Regulation EU/XXX should apply to the processing of this data for purposes other than the purposes of this Directive where such processing is authorized by Union or Member State law. In particular, the rules of Regulation EU/XXX should apply to the transmission of personal data for purposes outside the scope of this Directive. For the processing of personal data by a recipient who is not or is not acting as a competent authority within the meaning of this Directive and to whom personal data are lawfully disclosed by a competent authority, Regulation EU/XXX should apply. While implementing this Directive, Member States may also further specify the application of the rules of Regulation EU/XXX, subject to the conditions set out in Regulation EU/XXX.

(25) In order to be lawful, the processing of personal data under this Directive should be necessary for the performance of a task carried out in the public interest by a competent authority based on Union or Member State law for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security**.** These activities should cover the protection of vital interests of the data subject. The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require/order individuals to abide by the requests made. In this case**,** the data subject's consent (as defined in Regulation EU/XXX) should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the data subject's reaction could not be considered as a freely-given indication of his or her wishes. This should not preclude Member States to provide by law that the data subject may agree to the processing of his or her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or monitoring of the data subject's location with electronic tags for the execution of criminal penalties.

(25a) Member States should provide that where Union or Member States law applicable to the transmitting competent authority provides for specific conditions applicable in specific circumstances to the processing of personal data, such as for example the use of handling codes, the transmitting competent authority should inform the recipient to whom data are transmitted about such conditions and the requirement to respect them. Such conditions may for example include that the recipient to whom the data are transmitted does not transmit further the data or use it for other purposes or does not inform the data subject in case of a limitation to the right of information without the prior approval of the transmitting competent authority. These obligations apply also to transfers by the transmitting competent authority to recipients in third countries or international organisations. Member States should provide that that authority does not apply such conditions to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters IV and V of Title V of the Treaty on the Functioning of the European Union other than those applicable to similar data transmissions within the Member State of the transmitting competent authority.

(26) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms, deserve specific protection as the context of their processing may create important risks for the fundamental rights and freedoms. These data should also include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Directive does not imply an acceptance by the European Union of theories which attempt to determine the existence of separate human races. Such data should not be processed, unless processing is subject to appropriate safeguards for the rights and freedoms of the data subject laid down by law and is allowed in cases authorised by law; or if not already authorised by such a law the processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which is manifestly made public by the data subject. Appropriate safeguards for the rights and freedoms of the data subject may for example include the possibility to collect those data only in connection with other data on the individual concerned, to adequately secure the data collected, stricter rules on the access of staff of the competent authority to the data, or the prohibition of transmission of those data. Processing of such data should also be allowed by law when the data subject has explicitly agreed in cases where the processing of data is particularly intrusive for the persons. However, the agreement of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent authorities.

(27) The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her, which is based solely on automated processing, which produces adverse legal effects concerning him or her or significantly affects him or her. In any case, such processing should be subject to suitable safeguards, including specific information to the data subject and the right to obtain human intervention, in particular to express his or her point of view, to get an explanation of the decision reached after such assessment or the right to contest the decision. Profiling that results in discrimination against individuals on the basis of personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms, should be prohibited, under the conditions laid down in Articles 21 and 52 of the Charter of Fundamental Rights of the European Union.

(28) In order to exercise his or her rights, any information to the data subject should be easily accessible, including on the website of the controller, and easy to understand, requiring the use of clear and plain language. This information should be adapted to the needs of vulnerable persons such as children.

(29) Modalities should be provided for facilitating the data subject's exercise of his or her rights under the provisions adopted pursuant to this Directive, including mechanisms to request, free of charge, access to his or her personal data, as well as rectification, erasure and restriction. The controller should be obliged to respond to requests of the data subject without undue delay, unless the controller applies limitations to data subject rights in accordance with the rules of this Directive. Moreover, if requests are manifestly unfounded or excessive such as when the data subject unreasonably and repetitiously requests information or where the data subject abuses his or her right to receive information, for example, by providing false or misleading information when making the request, the controller may charge a reasonable fee or refuse to act on the request.

(29a) When the controller requests the provision of additional information necessary to confirm the identity of the data subject, this information should be processed only for this specific purpose and not stored longer than needed for this specific purpose.

(30) At least the following information should be made available to the data subject: the identity of the controller, the existence of the processing operation, the purposes of the processing, the right to lodge a complaint and the existence of the right to request from the controller access to and rectification, erasure or restriction of processing. This could take place on the website of the competent authority. In addition, in specific cases and in order to enable the exercise of his or her rights, the data subject should be informed of the legal basis of the processing and of how long the data will be stored, in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

(31) (…)

(32) A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing. Every data subject should therefore have the right to know about and obtain communication in particular of the purposes for which the data are processed, for what period, and which recipients receive the data, including in third countries. When this communication includes information as to the origin of the personal data, such information should not reveal the identity of natural persons, in particular confidential sources. For that right to be complied with, it is sufficient that the data subject be in possession of a full summary of those data in an intelligible form, that is to say a form which allows that data subject to become aware of those data and to verify that they are accurate and processed in compliance with this Directive, so that he or she may, where relevant, exercise the rights conferred on him or her by this Directive. Such a summary could be provided in the form of a copy of the personal data undergoing processing.

(33) Member States should be allowed to adopt legislative measures delaying, restricting or omitting the information to data subjects or restricting, wholly or partly, the access to their personal data to the extent that and as long as such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the individual concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others. The controller should assess, by way of a concrete and individual examination of each case, whether the right of access should be partially or completely restricted.

(34) Any refusal or restriction of access should in principle be set out in writing to the data subject and include the factual or legal reasons on which the decision is based.

(34a) Any restriction of the rights of the data subject must be in compliance with the Charter of Fundamental Rights of the European Union and with the European Convention on Human Rights, as interpreted by the case law of the Court of Justice of the European Union and the European Court of Human Rights respectively, and in particular respect the essence of those rights and freedoms.

(35) (…)

(36) A natural person should have the right to have inaccurate personal data concerning him or her rectified, in particular when pertaining to facts, and the right to erasure where the processing of such data is not in compliance with the provisions laid down in this Directive. However, the right to rectification should not affect, for example, the content of a witness testimony. A natural person should also have the right to restriction of processing when he or she contests the accuracy of personal data and its accuracy or inaccuracy cannot be ascertained or when the personal data have to be maintained for purpose of proof. In particular, personal data should be restricted instead of erased if in a specific case there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. In this case, restricted data should be processed only for the purpose which prevented their erasure**.** Methods to restrict processing of personal data could include, inter alia, moving the selected data to another processing system**,** for example for archiving purposes, or making the selected data unavailable. In automated filing systems the restriction of processing of personal data should in principle be ensured by technical means; the fact that the processing of personal data is restricted should be indicated in the system in such a way that it is clear that the processing of the personal data is restricted. Such rectification, erasure or restriction of processing should be communicated to recipients to whom the data have been disclosed and to the competent authorities from which the inaccurate data originated. The controllers should also abstain from further dissemination of such data.

(36a) Where the controller denies a data subject his or her right to information, access, rectification, erasure or restriction of processing, the data subject should have the right to request that the national supervisory authority verifies the lawfulness of the processing. The data subject should be informed of this right. When the supervisory authority acts on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications or reviews by the supervisory authority have taken place. The supervisory authority should also inform the data subject of the right to seek a judicial remedy.

(36aa) Where the personal data are processed in the course of a criminal investigation and court proceedings in criminal matters, the exercise of the rights to information, access, rectification, erasure and restriction of processing may be carried out in accordance with national rules on judicial proceedings.

(37) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate compliance of processing activities with this Directive. These measures should take into account the nature, scope, context and purposes of the processing and the risk for the rights and freedoms of individuals. The measures taken by the controller should include drawing up and implementing specific safeguards in respect of the treatment of personal data of vulnerable persons such as children.

(37a) Risks for the rights and freedoms of data subjects, of varying likelihood and severity, may result from data processing which could lead to physical, material or moral damage, in particular where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, unauthorized reversal of pseudonymisation, or any other significant economic or social disadvantage; or where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data in order to uniquely identify a person or data concerning health or sex life and sexual orientation or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable individuals, in particular children, are processed; where processing involves a large amount of personal data and affects a large number of data subjects.

(37b) The likelihood and severity of the risk should be determined in function of the nature, scope, context and purposes of the data processing. Risk should be evaluated according to an objective assessment, through which it is established whether data processing operations involve a high risk. A high risk is a particular risk of prejudice to the rights and freedoms of data subjects.

(38) The protection of the rights and freedoms of individuals with regard to the processing of personal data requires that appropriate technical and organisational measures are taken, to ensure that the requirements of this Directive are met. The implementation of such measures cannot depend solely on economic considerations. In order to be able to demonstrate compliance with this Directive, the controller should adopt internal policies and implement measures, which respect in particular the principles of data protection by design and data protection by default. Where the controller has carried out a data protection impact assessment pursuant to this Directive, the results should be taken into account when developing those measures and procedures. The measures could consist, inter alia, of the use of pseudonymisation, as soon as possible. The use of pseudonymisation for the purposes of this Directive can serve as a tool that could facilitate, in particular, the free flow of personal data within the Area of Freedom, Security and Justice.

(39) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Directive, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(39a) The carrying out of processing by a processor should be governed by a legal act including a contract binding the processor to the controller and stipulating, in particular, that the processor should act only on instructions from the controller. The processor should take into account the principle of data protection by design and by default.

(40) In order to demonstrate compliance with this Directive, the controller or processor should maintain records regarding all categories of personal data processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make these records, on request, available to it, so that it might serve for monitoring those processing operations. The controller or the processor processing personal data in non-automated processing systems should have in place effective methods of demonstrating the lawfulness of the data processing, of enabling self-monitoring and of ensuring data integrity and data security, such as logs or other forms of records.

(40a) Logs should be kept at least for operations in automated processing systems such as collection, alteration, consultation, disclosure including transfers, combination or erasure. The identification of the person who consulted or disclosed personal data should be logged and from this identification it could be possible to establish the justification of the processing operations. The logs should solely be used for the verification of the lawfulness of the data processing, self-monitoring, for ensuring data integrity and data security and criminal proceedings. Self-monitoring also includes internal disciplinary proceedings of competent authorities.

(40b) A data protection impact assessment should be carried out by the controller, where the processing operations are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, which should include, in particular, the envisaged measures, safeguards and mechanisms to ensure the protection of personal data and for demonstrating compliance with this Directive. Impact assessments should cover relevant systems and processes of personal data processing operations, but not individual cases.

(41) In order to ensure effective protection of the rights and freedoms of data subjects' the controller or processor should consult the supervisory authority, in certain cases, prior to the processing.

(41a) In order to maintain security and to prevent processing in breach of this Directive, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks, such as encryption. These measures should ensure an appropriate level of security including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risk and the nature of the personal data to be protected. In assessing data security risks, consideration should be given to the risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may, in particular, lead to physical, material or moral damage. The controller and processor should ensure that processing of personal data is not carried out by unauthorised persons.

(42) A personal data breach may, if not addressed in an adequate and timely manner, result in physical, material or moral damage to individuals such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage to the individual concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred and that this breach is likely to result in a risk for the rights and freedoms of the data subject, the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 72 hours. Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(43) The individuals should be notified without undue delay in case the personal data breach is likely to result in a high risk for the rights and freedoms of individuals, in order to allow them to take the necessary precautions. The notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities. For example, the need to mitigate an immediate risk of damage would call for a prompt notification of data subjects, whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay. Where avoiding obstruction of official or legal inquiries, investigations or procedures, avoiding prejudice to the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, protecting public security, protecting national security or protecting the rights and freedoms of others cannot be achieved by delaying or restricting the communication of a personal data breach to the individual concerned, such communication could, in exceptional circumstances, be omitted.

(44) The controller should designate a person who would assist the controller to monitor internal compliance with the provisions adopted pursuant to this Directive, except where a Member State decides to exempt courts and other independent judicial authorities when acting in their judicial capacity. This person may be a member of the existing staff of the controller who received special training in data protection law and practices in order to acquire expert knowledge in this field. The necessary level of expert knowledge should be determined, in particular, according to the data processing carried out and the protection required for the personal data processed by the controller. His or her task can be carried out on a part-time or full-time basis. A data protection officer may be appointed jointly by several controllers, taking into account their organisational structure and size, for example in case of shared resources in central units. This person can also be nominated to different positions within the structure of the relevant controllers. This person should help the controller and the employees processing personal data by informing and advising them on compliance with their relevant data protection obligations. Such data protection officers should be in a position to perform their duties and tasks in an independent manner in accordance with national law.

(45) Member States should ensure that a transfer to a third country or to an international organisation only takes place if it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer may only take place by competent authorities acting as controllers, except where processors are explicitly instructed to transfer on behalf of controllers. Such a transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level or protection, or when appropriate safeguards have been adduced or when derogations for specific situations apply. When personal data are transferred from the Union to controllers, processors or other recipients in third countries or international organisations, the level of protection of individuals guaranteed in the Union by this Directive should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation.

(45a) Where personal data are transferred from a Member State to third countries or international organisations, such a transfer should, in principle, take place only after the Member State from which the data were obtained has given its authorisation to the transfer. The interests of efficient law enforcement cooperation require, that where the nature of a threat to the public security of a Member State or a third country or to the essential interests of a Members State is so immediate as to render it impossible to obtain prior authorisation in good time, the competent authority should be able to transfer the relevant personal data to the third country or international organisation concerned without such a prior authorisation. Member States should provide that any specific conditions concerning the transfer should be communicated to third countries and/or international organisations. Onward transfers of personal data should be subject to the prior authorisation of the competent authority that carried out the original transfer. When deciding on a request for authorisation of an onward transfer, the competent authority that carried out the original transfer should take due account of all relevant factors, including the seriousness of the offence, the specific conditions attached and the purpose for which the data was originally transferred, the nature and conditions of the execution of the criminal penalty, and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred. The competent authority that carried out the original transfer may also subject the onward transfer to specific conditions. Such specific conditions can be described, for example, in handling codes.

(46) The Commission may decide with effect for the entire Union that certain third countries, or a territory or one or more specified sectors within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such a level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any specific authorisation, except when another Member State from which the data were obtained has to give its authorisation to the transfer.

(47) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or of a specified sector within a third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision relating to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees that ensure an adequate level of protection essentially equivalent to that guaranteed within the Union, in particular when data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision, provide for cooperation mechanisms with the European data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(47a) Apart from the international commitments the third country or international organisation has entered into, the Commission should also take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult with the European Data Protection Board when assessing the level of protection in third countries or international organisations. The Commission should also take into account any relevant Commission adequacy decision adopted in accordance with Article 41 of Regulation (EU) XXX.

(47b) The Commission should monitor the functioning of decisions on the level of protection in a third country or a territory or a specified sector within a third country, or an international organisation. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. This periodic review should be made in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation.

(48) The Commission should equally be able to recognise that a third country, or a territory or a specified sector within a third country, or an international organisation, no longer ensures an adequate level of data protection. Consequently, the transfer of personal data to that third country or international organisation should be prohibited unless the requirements of Articles 35 or36 are fulfilled. Provision should be made for procedures for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(49) Transfers not based on such an adequacy decision should only be allowed where appropriate safeguards have been adduced in a legally binding instrument, which ensure the protection of personal data, or where the controller has assessed all the circumstances surrounding the data transfer and, based on this assessment, considers that appropriate safeguards with respect to the protection of personal data exist. Such legally binding instruments could, for example, be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and may be enforced by their data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress**.** The controller may take into account cooperation agreements concluded between Europol or Eurojust and third countries which allow for the exchange of personal data when carrying out the assessment of all the circumstances surrounding the data transfer. The controller may also take into account that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition the controller should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman-treatment. While these conditions could be considered as appropriate safeguards allowing the transfer of data, the controller may require additional safeguards.

(49aa) Where no adequacy decision or appropriate safeguards exist, a transfer or a category of transfers could only take place in specific situations, if necessary, in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides, or where it is necessary for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or necessary in an individual case for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of public security, or necessary in an individual case for the establishment, exercise or defence of legal claims**.** Those derogations should be interpreted restrictively and should not allow frequent, massive and structural transfers of personal data and should not allow large-scale transfers of data but should be limited to data strictly necessary. Such transfers should be documented and should be made available to the supervisory authority on request in order to monitor the lawfulness of the transfer.

(49b) Competent authorities of Member States are applying bilateral or multilateral international agreements in force, concluded with third countries in the field of judicial co-operation in criminal matters and police co-operation, for the exchange of relevant information to allow them to perform their legally assigned tasks. In principle, this takes place through, or at least with, the cooperation of the competent authorities of the concerned third countries, sometimes even in the absence of a bilateral or multilateral international agreement. However, in specific individual cases, it may occur that the regular procedures requiring contacting the competent authority in the third country would be ineffective or inappropriate, in particular because the transfer could not be carried out in a timely manner, or because the competent authority in the third country does not respect the rule of law or international human rights norms and standards, so that competent authorities of Member States could decide to transfer personal data directly to recipients established in third countries. This may be the case where there is an urgent need to transfer personal data to save the life of a person who is in danger of becoming a victim of a criminal offence or in the interest of preventing an imminent perpetration of a crime, including terrorism. Even if this transfer between competent authorities and recipients established in third countries should only take place in specific individual cases, this Directive should provide for conditions to regulate such cases. These provisions should not be considered as derogations to any existing bilateral or multilateral international agreements in the field of judicial co-operation in criminal matters and police co-operation. These rules should apply in addition to the other rules of the Directive, in particular those on the lawfulness of processing and of Chapter V.

(50) When personal data move across borders it may put at increased risk the ability of individuals to exercise data protection rights to protect themselves from the unlawful use or disclosure of that data. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers and inconsistent legal regimes. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information with their foreign counterparts.

(51) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions adopted pursuant to this Directive and contribute to their consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data. For that purpose, the supervisory authorities should co-operate with each other and with the Commission.

(52) Member States may entrust a supervisory authority already established under Regulation EU/XXX with the responsibility for the tasks to be performed by the national supervisory authorities to be established under this Directive.

(53) Member States should be allowed to establish more than one supervisory authority to reflect their constitutional, organisational and administrative structure. Each supervisory authority should be provided with the financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(53a) Supervisory authorities should be subject to independent control or monitoring mechanisms regarding their financial expenditure, provided that this financial control does not affect their independence.

(54) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government or the head of State of the Member State based on a proposal from the government or a member of the government, or the parliament or its chamber, or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. In order to ensure the independence of the supervisory authority, the staff should be chosen by the supervisory authority which may include an intervention by an independent body entrusted by Member State law.

(55) While this Directive applies also to the activities of national courts and other judicial authorities, the competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. This exemption should be limited to judicial activities in court cases and not apply to other activities where judges might be involved in accordance with national law. Member States may also provide that the competence of the supervisory authority may not cover the processing of personal data of other independent judicial authorities when acting in their judicial capacity, for example public prosecutors office. In any event, the compliance with the rules of this Directive by the courts and other independent judicial authorities should always be subject to independent supervision in accordance with Article 8 (3) of the Charter of Fundamental Rights of the European Union.

(56) Each supervisory authority should deal with complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.

(57) In order to ensure effective, reliable and consistent monitoring of compliance with and enforcement of this Directive throughout the Union pursuant to the Treaty as interpreted by the Court of Justice of the European Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including investigative, corrective, and advisory powers which constitute necessary means to perform their tasks. However, their powers should not interfere with specific rules set out for criminal proceedings, including investigation and prosecution of criminal offences, or the independence of the judiciary. Without prejudice to the powers of prosecutorial authorities under national law, supervisory authorities should also have the power to bring infringements of this Directive to the attention of the judicial authorities and/or to engage in legal proceedings. The powers of supervisory authorities should be exercised in conformity with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Directive, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure that would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigative powers as regards access to premises should be exercised in accordance with specific requirements in national law, such as the requirement to obtain a prior judicial authorisation. The adoption of a legally binding decision should be subject to judicial review in the Member State of the supervisory authority that adopted the decision.

(58) The supervisory authorities should assist one another in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive.

(59) The European Data Protection Board established by Regulation EU/XXX should contribute to the consistent application of this Directive throughout the Union, including advising the Commission and promoting the co-operation of the supervisory authorities throughout the Union.

(60) Every data subject should have the right to lodge a complaint with a single supervisory authority and have the right to an effective judicial remedy in accordance with Article 47 of the Charter of Fundamental Rights of the European Union, if the data subject considers that his or her rights under provisions adopted pursuant to this Directive are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The competent supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can be completed also electronically, without excluding other means of communication.

(61) Each natural or legal person should have the right to an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning this person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, this right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with the national law of that Member State. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it.

(62) Where a data subject considers that his or her rights under this Directive are infringed, he or she should have the right to mandate a body, which aims to protect the rights and interests of data subjects in relation to the protection of their personal data and is constituted according to the law of a Member State, to lodge a complaint on his or her behalf with a supervisory authority and to exercise the right to a judicial remedy. The right of representation of data subjects should be without prejudice to national procedural law which may require mandatory representation of data subjects by a lawyer, as defined by Directive 77/249/EEC, before national courts.

(63) (…)

(64) Any damage which a person may suffer as a result of processing that is not in compliance with the provisions adopted pursuant to this Directive should be compensated by the controller or any other authority competent under national law. The concept of damage should be broadly interpreted in the light of the case law of the Court of Justice of the European Union in a manner which fully reflects the objectives of this Directive. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. When reference is made to a processing that is unlawful or not in compliance with the provisions adopted pursuant to this Directive it also covers processing that is not in compliance with implementing acts adopted in accordance with this Directive. Data subjects should receive full and effective compensation for the damage they have suffered.

(65) Penalties should be imposed on any natural or legal person, whether governed by private or public law, that fails to comply with this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and must take all measures to implement the penalties.

(66) (…)

(67) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission for: the adequate level of protection afforded by a third country or a territory or a specified sector within that third country or an international organisation; and for the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers.[7]

(68) The examination procedure should be used for the adoption of implementing acts on the adequate level of protection afforded by a third country or a territory or a specified sector within that third country or an international organisation; the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, given that those acts are of a general scope.

(69) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a specified sector within that third country or an international organisation which no longer ensure an adequate level of protection, imperative grounds of urgency so require.

---

[7] OJ L 55, 28.2.2011, p. 13.

(70) Since the objectives of this Directive, namely to protect the fundamental rights and freedoms of data subjects and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent authorities within the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective. Member States may provide for higher standards than those established in this Directive.

(71) Framework Decision 2008/977/JHA should be repealed by this Directive.

(72) Specific provisions of acts of the Union adopted in the field of judicial co-operation in criminal matters and police co-operation which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected, such as, for example, the specific provisions concerning the protection of personal data applied pursuant to Council Decision 2008/615/JHA,[8] or Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01).[9] Since Article 8 of the Charter and Article 16 TFEU require that the fundamental right to the protection of personal data should be ensured in a consistent manner through the Union, the Commission should evaluate the situation with regard to the relationship between this Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, in order to assess the need for alignment of these specific provisions with this Directive. Where appropriate, the Commission should make proposals with a view to ensuring consistent legal rules relating to the processing of personal data.

---

[8] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1.

[9] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000, p. 1.

(73) In order to ensure a comprehensive and coherent protection of personal data in the Union, international agreements concluded by Member States prior to the entry into force of this Directive, and which are in compliance with the relevant Union law applicable prior to the entry into force of this Directive, should remain in force until amended, replaced, or revoked.

(73a) Member States should be allowed a period of not more than two years from the entry into force to implement this Directive. Processing already under way on the date of the entry into force of this Directive should be brought in conformity with this Directive within the period of two years after which this Directive enters into force. However, where such processing is in compliance with the Union law applicable prior to the entry into force of this Directive, the requirements of this Directive concerning the prior consultation of the supervisory authority should not apply to the processing operations already under way prior to the entry into force of this Directive, given that these requirements, by their very nature, are to be met prior to the processing. Where Member States use the longer implementation period expiring 7 years after the date of entry into force of this Directive for meeting the logging obligations for automated processing systems set up prior to the date of entry into force of this Directive, the controller or the processor should have in place effective methods of demonstrating the lawfulness of the data processing, of enabling self-monitoring and of ensuring data integrity and data security, such as logs or other forms of records.

(74) This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011.[10]

[10] OJ L 335, 17.12.2011, p. 1.

(75) In accordance with Article 6a of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, the United Kingdom and Ireland are not bound by the rules laid down in this Directive which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the Treaty on the Functioning of the European Union where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial co-operation in criminal matters or police co-operation which require compliance with the provisions laid down on the basis of Article 16 of the Treaty on the Functioning of the European Union.

(76) In accordance with Articles 2 and 2a of the Protocol on the position of Denmark, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not bound by the rules laid down in this Directive or subject to their application which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the Treaty on the Functioning of the European Union. Given that this Directive builds upon the Schengen acquis, under Title V of Part Three of the Treaty on the Functioning of the European Union, Denmark shall, in accordance with Article 4 of that Protocol, decide within six months after adoption of this Directive whether it will implement it in its national law.

(77) As regards Iceland and Norway, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis.[11]

[11] OJ L 176, 10.7.1999, p. 36.

(78) As regards Switzerland, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis.[12]

(79) As regards Liechtenstein, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis.[13]

(80) This Directive respects the fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaty, notably the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on these rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

(81) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents,[14] Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

---

[12] OJ L 53, 27.2.2008, p. 52.
[13] OJ L 160 of 18.6.2011, p. 21.
[14] OJ C 369, 17.12.2011, p. 14.

(82) This Directive should not preclude Member States from implementing the exercise of the rights of data subjects on information, access, rectification, erasure and restriction of their personal data processed in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure.

## CHAPTER I
## GENERAL PROVISIONS

*Article 1*
***Subject matter and objectives***

1. This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

1a. This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.

2. In accordance with this Directive, Member States shall:

   (a) protect the fundamental rights and freedoms of individuals and in particular their right to the protection of personal data; and

   (b) ensure that the exchange of personal data by competent authorities within the Union, where such exchange is required by Union or national law, is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

*Article 2*
***Scope***

1. This Directive applies to the processing of personal data by competent authorities for the purposes set out in Article 1(1).

2. This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

3. This Directive shall not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Union institutions, bodies, offices and agencies.

*Article 3*
***Definitions***

For the purposes of this Directive:

(1) 'personal data' means any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(2) (…)

(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination**,** restriction, erasure or destruction;

(4) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(4a) 'pseudonymisation' means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person;

(5) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(6) 'controller' means the competent authority, which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by Union or Member State law, the controller or the specific criteria for his nomination may be designated by Union or by Member State law;

(7) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(8) 'recipient' means a natural or legal person, public authority, agency or any other body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive data in the framework of a particular inquiry in accordance with national law shall not be regarded as recipients; the processing of these data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(10) 'genetic data' means all personal data, relating to genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question;

(11) 'biometric data' means any personal data resulting from specific technical processing relating to the physical physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data;

(12) 'data concerning health’ means data related to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status;

(12a) 'profiling' means any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

(13) (…)

(14) 'competent authority' means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by national law to exercise public authority and public powers for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(15) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 39.

(16) 'international organisation' means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries.

## CHAPTER II
## PRINCIPLES

*Article 4*

***Principles relating to personal data processing***

1. Member States shall provide that personal data must be:

   (a) processed lawfully and fairly;

   (b) collected for specified, explicit and legitimate purposes and not processed in a way incompatible with those purposes;

   (c) adequate, relevant, and not excessive in relation to the purposes for which they are processed;

   (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

   (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

   (f) (…)

   (fb) processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. Processing by the same or another controller for other purposes set out in Article 1 (1) than the one for which the data are collected shall be permitted in so far as:

   (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and

(b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.

3. Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use for the purposes set out in Article 1 (1), subject to appropriate safeguards for the rights and freedoms of data subjects.

4. The controller shall be responsible for and be able to demonstrate compliance with paragraphs 1, 2 and 3.

*Article 4b*

***Time limits of storage and review***

Member States shall provide that appropriate time limits are established for the erasure of personal data or for a periodic review of the need for the storage of the data. Procedural measures shall ensure that these time limits are observed.

*Article 5*

***Distinction between different categories of data subjects***

1. Member States shall provide that, where applicable and as far as possible, the controller makes a clear distinction between personal data of different categories of data subjects, such as:

   (a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;

   (b) persons convicted of a criminal offence;

   (c) victims of a criminal offence, or persons with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence; and

(d) third parties to the criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or a person who can provide information on criminal offences, or a contact or associate to one of the persons mentioned in (a) and (b).

(e) (…)

*Article 6*

***Distinction of personal data and verification of quality of data***

1. Member States shall ensure that, as far as possible, personal data based on facts are distinguished from personal data based on personal assessments.

2. Member States shall provide that the competent authorities shall take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, each competent authority shall as far as practicable verify the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of personal data, necessary information shall be added which enables the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up-to-date.

3. If it emerges that incorrect personal data have been transmitted or the data have been unlawfully transmitted, the recipient must be notified without delay. In such case the personal data must be rectified, erased or restricted in accordance with Article 15.

*Article 7*

***Lawfulness of processing***

1. Member States shall provide that the processing of personal data is lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and is based on Union or Member State law.

   (a) (…)

   (b) (...)

   (c) (...)

   (d) (...)

1a. Member State law regulating the processing of personal data within the scope of this Directive shall specify at least the objectives, the personal data to be processed and the purposes of the processing.

*Article 7a*

***Specific processing conditions***

1. Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for other purposes than those set out in Article 1(1) unless such processing is authorized by Union or Member State law. In these cases, Regulation EU/XXX shall apply for this processing unless the processing is carried out in an activity which falls outside the scope of Union law.

1a. Where competent authorities are entrusted by Member State law with the performance of tasks other than for the purposes set out in Article 1 (1), Regulation EU/XXX shall apply to the processing for such purposes, including, for archiving in the public interest, scientific, statistical or historical use, unless the processing is carried out in an activity which falls outside the scope of Union law.

1b. Member States shall provide that where Union or Member State law applicable to the transmitting competent authority provides specific conditions for the processing of personal data, the transmitting competent authority shall inform the recipient to whom the data are transmitted about such conditions and the requirement to respect them.

2. Member States shall provide that the transmitting competent authority does not apply conditions pursuant to paragraph 1b to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters IV and V of Title V of the Treaty on the Functioning of the European Union other than those applicable to similar transmissions of data within the Member State of the transmitting competent authority.

*Article 8*

***Processing of special categories of personal data***

1. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data in order to uniquely identify a person or data concerning health or sex life and sexual orientation shall only be allowed when strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject and only if:

   (a) authorised by Union or Member State law; or;

   (b) to protect the vital interests of the data subject or of another person; or

   (c) the processing relates to data which are manifestly made public by the data subject.

2. (…)

*Article 9*

***Automated individual decision making***

1. Member States shall provide that a decision based solely on automated processing, including, profiling, which produces an adverse legal effect for the data subject or significantly affects him or her shall be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

2. Decisions referred to in paragraph 1 shall not be based on special categories of personal data referred to in Article 8, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

2b. Profiling that results in discrimination against individuals on the basis of special categories of personal data referred to in Article 8 shall be prohibited, in accordance with Union law.

## CHAPTER III
## RIGHTS OF THE DATA SUBJECT

*Article 10*

***Communication and modalities for exercising the rights of the data subject***

1. (…)

2. Member States shall provide that the controller takes reasonable steps to provide any information referred to in Article 10a and any communication under Articles 9, 12 to 17 and 29 relating to the processing of personal data to the data subject in a concise, intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including electronically. As a general rule the controller shall provide the information in the same form as the request.

3. Member States shall provide that the controller facilitates the exercise of the rights of the data subject under Articles 9 and 12 to 17.

4. Member States shall provide that the controller informs the data subject in writing about the follow-up given to his or her request without undue delay.

5. Member States shall provide that the information provided under Article 10a and any communication and any actions taken under Articles 9,12 to 17 and 29 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may charge a reasonable fee taking into account the administrative costs for providing the information or the communication or taking the action requested, or the controller may refuse to act on the request. In these cases, the controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

5a. Where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 12 and 15, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

*Article 10a*

***Information to the data subject***

1. Member States shall provide that the controller makes available to the data subject at least the following information:

   (a) the identity and the contact details of the controller; the controller shall also include the contact details of the data protection officer, if any;

   (b) the purposes of the processing for which the personal data are intended;

   (c) the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority;

   (d) the existence of the right to request from the controller access to and rectification, erasure or restriction of processing of the personal data concerning the data subject.

2. Member States shall provide by law that the controller gives to the data subject, in specific cases, the following information in addition to those referred to in paragraph 1, in order to enable the exercise of his or her rights:

   (a) the legal basis of the processing;

   (b) the period for which the personal data will be stored, or if not possible, the criteria used to determine this period;

   (c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations;

   (d) where necessary, further information, in particular where the data are collected without the knowledge of the data subject.

3. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that and as long as such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the individual concerned:

(a) to avoid obstructing official or legal inquiries, investigations or procedures;

(b) to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) to protect public security;

(d) to protect national security;

(e) to protect the rights and freedoms of others.

4. Member States may adopt legislative measures in order to determine categories of data processing which may wholly or partly fall under the exemptions of paragraph 3.

*Article 11*

(…)

*Article 12*

***Right of access for the data subject***

1. Subject to Article 13, Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where such personal data are being processed, access to the data and the following information:

   (a) the purposes of the processing as well as the legal basis for the processing;

   (b) the categories of personal data concerned;

   (c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;

   (d) where possible, the envisaged period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period;

   (e) the existence of the right to request from the controller rectification, erasure or restriction of processing of personal data concerning the data subject;

   (f) the right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority;

   (g) communication of the personal data undergoing processing and of any available information as to their origin.

2. (…)

*Article 13*

***Limitations to the right of access***

1. Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent and for the envisaged period that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the individual concerned:

   (a) to avoid obstructing official or legal inquiries, investigations or procedures;

   (b) to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

   (c) to protect public security;

   (d) to protect national security;

   (e) to protect the rights and freedoms of others.

2. Member States may adopt legislative measures in order to determine categories of data processing which may wholly or partly fall under the exemptions of paragraph 1.

3. In cases referred to in paragraph 1 and 2, Member States shall provide that the controller informs the data subject, without undue delay, in writing of any refusal or restriction of access, and of the reasons for the refusal or the restriction. This information may be omitted where the provision of such information would undermine a purpose under paragraph 1. Member States shall provide that the controller informs the data subject of the possibilities of lodging a complaint with a supervisory authority or seeking a judicial remedy.

4. Member States shall ensure that the controller documents the factual or legal reasons on which the decision is based. That information shall be made available to the supervisory authorities.

*Article 14*

*(...)*

*Article 15*

***Right to rectification, erasure and restriction of processing***

1. Member States shall provide for the right of the data subject to obtain from the controller without undue delay the rectification of personal data relating to him or her which are inaccurate. Having regard to the purpose of the processing concerned, Member States shall provide that the data subject has the right to obtain completion of incomplete personal data, including by means of providing a supplementary statement.

1a. Member States shall provide for the obligation of the controller to erase personal data without undue delay and for the right of the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay where the processing does not comply with the provisions adopted pursuant to Articles 4, 7 and 8 of this Directive, or where the data have to be erased for compliance with a legal obligation to which the controller is subject.

1b. Instead of erasure, the controller shall restrict the processing of the personal data where:

(a) the accuracy of the personal data is contested by the data subject and the accuracy or inaccuracy cannot be ascertained; or

(b) the personal data have to be maintained for the purposes of proof.

1c. Where processing of personal data is restricted pursuant to point (a) of paragraph (1b), the controller shall inform the data subject before lifting the restriction on processing.

2. Member States shall provide that the controller informs the data subject in writing of any refusal of rectification, erasure or restriction of the processing, and of the reasons for the refusal. Member States may adopt legislative measures restricting, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the individual concerned in order:

(a) to avoid obstructing official or legal inquiries, investigations or procedures;

(b) to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) to protect public security;

(d) to protect national security;

(e) to protect the rights and freedoms of others.

Member States shall provide that the controller informs the data subject of the possibilities of lodging a complaint with a supervisory authority or seeking a judicial remedy.

2b. Member States shall provide that the controller communicates the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originate.

3. Member States shall provide that in the cases referred to in paragraphs 1, 1a, 1b and 1c the controller shall notify the recipients and that the recipients shall rectify, erase or restrict the processing of the personal data under their responsibility.

*Article 15a*

***Exercise of rights by the data subject and verification by the supervisory authority***

1. In cases referred to in Article 10a(3), Article 13(3) and Article 15(2) Member States shall adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authority.

1a. Member States shall provide that the controller informs the data subject of the possibility to exercise his or her rights through the supervisory authority pursuant to paragraph 1.

2. When the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place. The supervisory authority shall also inform the data subject of his or her right to seek a judicial remedy.

*Article 16*

*(...)*

*Article 17*

***Rights of the data subject in criminal investigations and proceedings***

Member States may provide that the exercise of the rights referred to in Articles 10a, 12 and 15 is carried out in accordance with national law where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings.

## CHAPTER IV
## CONTROLLER AND PROCESSOR

### SECTION 1
### GENERAL OBLIGATIONS

*Article 18*

***Obligations of the controller***

1. Member States shall provide that, taking into account the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of individuals, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Directive. These measures shall be reviewed and updated, where necessary.

1a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

2. (…)

3. (…)

*Article 19*

***Data protection by design and by default***

1. Member States shall provide that, having regard to the state of the art and the cost of implementation and taking account of the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing, in order to meet the requirements of this Directive and protect the rights of data subjects.

2. Member States shall provide that the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed; this applies to the amount of data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of individuals.

*Article 20*

***Joint controllers***

1. Member States shall provide that, where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers. They shall, in a transparent manner, determine their respective responsibilities for compliance with the obligations under this Directive, in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information referred to in Article 10a, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement shall designate the point of contact for data subjects. Member States may designate which of the joint controllers can act as a single point of contact for data subjects to exercise their rights.

1a. Irrespective of the terms of the arrangement referred to in paragraph 1, Member States may provide that the data subject may exercise his or her rights under the provisions adopted pursuant to this Directive in respect of and against each of the controllers.

*Article 21*

***Processor***

1. Member States shall provide that where a processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Directive and ensure the protection of the rights of the data subject.

1a. Member States shall provide that the processor shall not enlist another processor without the prior specific or general written authorisation of the controller. In the latter case, the processor shall always inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes.

2. Member States shall provide that the carrying out of processing by a processor shall be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the controller and stipulating in particular that the processor shall:

(a) act only on instructions from the controller;

(b) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) assist the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;

(d) at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of data processing services, and delete existing copies unless Union or Member State law requires storage of the data;

(e) make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article;

(f) respect the conditions referred to in paragraphs 1a and 2 for enlisting another processor.

2a. The contract or the other legal act referred to in paragraph 2 shall be in writing, including in an electronic form.

3. If a processor in breach of this Directive determines the purposes and means of data processing, the processor shall be considered to be a controller in respect of that processing.

*Article 22*

***Processing under the authority of the controller and processor***

Member States shall provide that the processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.

*Article 23*

***Records of processing activities***

1. Member States shall provide that each controller shall maintain a record of all categories of personal data processing activities under their responsibility. This record shall contain the following information:

   (a) the name and contact details of the controller, any joint controller and the data protection officer;

   (b) the purposes of the processing;

   (c) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries;

   (ca) a description of categories of data subjects and of the categories of personal data;

   (cb) where applicable, the use of profiling;

   (d) where applicable, the categories of transfers of personal data to a third country or an international organisation;

   (da) an indication of the legal basis of the processing operation, including transfers, for which the data are intended;

   (e) where possible, the envisaged time limits for erasure of the different categories of data;

   (f) where possible, a general description of the technical and organisational security measures referred to in Article 27(1).

2. (…)

2a. Member States shall provide that each processor shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors, of each controller on behalf of which the processor is acting and the data protection officer, if any;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation, where explicitly instructed to do so by the controller;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 27(1).

2b. The records referred to in paragraph 1 and 2a shall be in writing, including in an electronic form.

3. On request, the controller and the processor shall make the record available to the supervisory authority.

*Article 24*

***Logging***

1. Member States shall ensure that logs are kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination or erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and as far as possible the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such data.

2. The logs shall be used solely for verification of the lawfulness of the data processing, self-monitoring, ensuring data integrity and data security, and for criminal proceedings.

2a. The controller and the processor shall make the logs available, on request, to the supervisory authority.

*Article 25*

***Cooperation with the supervisory authority***

1. Member States shall provide that the controller and the processor shall co-operate, on request, with the supervisory authority in the performance of its tasks.

2. (…)

*Article 25a*

***Data Protection impact assessment***

1. Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk for the rights and freedoms of individuals, Member States shall provide that the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate the compliance with the provisions in this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

*Article 26*

***Prior consultation of the supervisory authority***

1. Member States shall ensure that the controller or the processor consults the supervisory authority prior to the processing of personal data which will form part of a new filing system to be created, where:

   (a) a data protection impact assessment as provided for in Article 25a indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or

   (b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk for the rights and freedoms of data subjects.

1a. Member States shall ensure that the supervisory authority is consulted during the preparation of a proposal for a legislative measure to be adopted by a national parliament or of a regulatory measure based on such a legislative measure, which relates to the processing of personal data.

2. Member States shall provide that the supervisory authority may establish a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.

2a. Member States shall provide that the controller shall provide the supervisory authority with the data protection impact assessment pursuant to Article 25a and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

3. Member States shall provide that where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would not comply with the provisions adopted pursuant to this Directive, in particular where the controller has insufficiently identified or mitigated the risk, it shall, within a maximum period of six weeks, following the request for consultation give advice to the data controller, and where applicable the processor in writing, and may use any of its powers referred to in Article 46. This period may be extended for a further month, taking into account the complexity of the intended processing. Where the extended period applies, the controller, and, where applicable, the processor shall be informed within one month of receipt of the request including of the reasons for the delay.

## SECTION 2
## DATA SECURITY

*Article 27*

***Security of processing***

1. Member States shall provide that, having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the controller and the processor shall implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of data referred to in Article 8.

2. In respect of automated data processing, each Member State shall provide that the controller or processor, following an evaluation of the risks, implements measures designed to:

   (a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);

   (b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

   (c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

   (d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);

   (e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);

   (f) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input (input control);

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);

(i) ensure that installed systems may, in case of interruption, be restored (recovery);

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored personal data cannot be corrupted by means of a malfunctioning of the system (integrity).

3. (…)

*Article 28*

***Notification of a personal data breach to the supervisory authority***

1. Member States shall provide that in the case of a personal data breach, the controller notifies without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) (…)

(d) describe the likely consequences of the personal data breach;

(e) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects.

3a. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

4. Member States shall provide that the controller shall document any personal data breaches referred to in paragraph 1, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article.

4a. Member States shall provide that where the data breach involves personal data that have been transmitted by or to the controller of another Member State, the information referred to in paragraph 3 shall be communicated to the controller of this Member State without undue delay.

5. (…)

6. (…)

*Article 29*

***Communication of a personal data breach to the data subject***

1. Member States shall provide that when the personal data breach is likely to result in a high risk for the rights and freedoms of individuals, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe in clear and plain language the nature of the personal data breach and shall contain at least the information and the recommendations provided for in Article 28(3) (b), (d) and (e).

3. The communication to the data subject referred to in paragraph 1 shall not be required if:

(a) the controller has implemented appropriate technological and organisational protection measures, and that those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption; or

(b) the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; or

(c) it would involve a disproportionate effort. In such case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.

3a. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the breach to result in a high risk, may require it to do so, or may decide that any of the conditions referred to in paragraph 3 are met.

4. The communication to the data subject referred to in paragraph 1 may be delayed, restricted or omitted subject to the conditions and on the grounds referred to in Article 10a (3).

## SECTION 3
## DATA PROTECTION OFFICER

*Article 30*

***Designation of the data protection officer***

1. Member States shall provide that the controller designates a data protection officer. Member States may exempt courts and other independent judicial authorities when acting in their judicial capacity from this obligation.

2. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 32.

3. A single data protection officer may be designated for several competent authorities, taking account of their organisational structure and size.

3a. Member States shall provide that the controller shall publish the contact details of the data protection officer and communicate these to the supervisory authority.

*Article 31*

***Position of the data protection officer***

1. Member States shall provide that the controller shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.

2. The controller shall support the data protection officer in performing the tasks referred to in Article 32 by providing resources necessary to carry out these tasks, as well as, access to personal data and processing operations, and to maintain his or her expert knowledge.

*Article 32*

***Tasks of the data protection officer***

Member States shall provide that the controller entrusts the data protection officer at least with the following tasks:

(a) to inform and advise the controller and the employees who are processing personal data of their obligations pursuant to this Directive and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Directive, with other Union or Member State data protection provisions and with the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations, and the related audits;

(c) (…)

(d) (…)

(e) (…)

(f) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 25a;

(g) to cooperate with the supervisory authority;

(h) to act as the contact point for the supervisory authority on issues related to the processing of personal data, including the prior consultation referred to in Article 26, and consult, as appropriate, on any other matter.

## CHAPTER V
## TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

*Article 33*

***General principles for transfers of personal data***

1. Member States shall provide that any transfer by competent authorities of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation including for onward transfers to another third country or international organisation, may only take place, subject to compliance with the national provisions adopted pursuant to other provisions of this Directive, if the conditions laid down in this Chapter are complied with, namely:

(a) the transfer is necessary for the purposes set out in Article 1 (1); and

(b) (…);

(c) the data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in Article 1(1); and

(d) in case personal data are transmitted or made available from another Member State, that Member State has given its prior authorisation to the transfer in compliance with its national law; and

(e) the Commission has decided pursuant to Article 34 that the third country or international organisation in question ensures an adequate level of protection, or in the absence of an adequacy decision pursuant to Article 34, where appropriate safeguards are adduced or exist pursuant to Article 35, or both in the absence of an adequacy decision pursuant to Article 34 and of appropriate safeguards in accordance with Article 35, derogations for specific situations apply pursuant to Article 36;

(ea) in case of an onward transfer to another third country or international organisation, the competent authority that carried out the original transfer or another competent authority of the same Member State authorises the onward transfer, after taking into due account all relevant factors, including the seriousness of the offence, the purpose for which the data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

2. Member States shall provide that transfers without the prior authorisation by another Member State in accordance with point (d) shall be permitted only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

3a. All provisions in this Chapter shall be applied in order to ensure that the level of protection of individuals guaranteed by this Directive shall not be undermined.

*Article 34*

***Transfers with an adequacy decision***

1. Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, or a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectorial, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of this legislation, data protection rules, professional rules and security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that country or international organisation, jurisprudential precedents, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with data protection rules, including adequate sanctioning powers for assisting and advising data subjects in exercising their rights and for co-operation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide that a third country, or a territory or one or more specified sectors within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. The implementing act shall provide a mechanism for periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 57(2).

4. (…)

4a. The Commission shall, on an on-going basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3, decide that a third country, or a territory or a specified sector within that third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 and, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 without retro-active effect. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 57(2), or, in cases of extreme urgency, in accordance with the procedure referred to in Article 57(3).

5a. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

6. Member States shall provide that a decision pursuant to paragraph 5 is without prejudice to transfers of personal data to the third country, or the territory or specified sector within that third country, or the international organisation in question pursuant to Articles 35 to 36.

7. The Commission shall publish in the Official Journal of the European Union and on its website a list of those third countries, territories and specified sectors within a third country and international organisations where it has decided that an adequate level of protection is or is no longer ensured.

8. (…)

*Article 35*

***Transfers by way of appropriate safeguards***

1. In the absence of a decision pursuant to Article 34, Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where:

   (a) appropriate safeguards with respect to the protection of personal data have been adduced in a legally binding instrument; or

   (b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with respect to the protection of personal data.

1a. The controller shall inform the supervisory authority about categories of transfers under point (b) of paragraph (1).

2. When a transfer is based on point (b) of paragraph 1, such a transfer must be documented and the documentation must be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the data transferred.

*Article 36*

***Derogations for specific situations***

1. In the absence of an adequacy decision pursuant to Article 34, or of appropriate safeguards pursuant to Article 35, Member States shall provide that a transfer or a category of transfers of personal data to a third country or an international organisation may take place only on the condition that:

   (a) the transfer is necessary in order to protect the vital interests of the data subject or another person; or

   (b) the transfer is necessary to safeguard legitimate interests of the data subject, where the law of the Member State transferring the personal data so provides; or

(c) the transfer of the data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country; or

(d) the transfer is necessary in individual cases for the purposes set out in Article 1 (1); or

(e) the transfer is necessary in an individual case for the establishment, exercise or defence of legal claims relating to the purposes set out in Article 1 (1).

2. Personal data shall not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer set out in points (d) and (e) of paragraph 1.

3. When a transfer is based on paragraph 1, such a transfer must be documented and the documentation must be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the data transferred.

*Article 36aa*

***Transfer of personal data to recipients established in third countries***

1. By way of derogation from Article 33 (1) (c) and without prejudice to any international agreement referred to in paragraph 2, Union or Member State law may provide that the competent authorities referred to in Article 3 (14)(a) may, in individual and specific cases, transfer personal data directly to recipients established in third countries only if the other provisions of this Directive are complied with and the following conditions are fulfilled:

(a) the transfer is strictly necessary for the performance of a task of the transferring competent authority as provided for by Union or Member State law for the purposes set out in Article 1(1); and

(b) the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand; and

(c) the transferring competent authority considers that the transfer to an authority competent for the purposes referred to in Article 1(1) in the third country is ineffective or inappropriate, in particular because it cannot be achieved in good time; and

(d) the competent authority in the third country is informed without undue delay, unless this is ineffective or inappropriate; and

(e) the transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data shall only be processed by the latter where such processing is necessary.

2. An international agreement referred to in paragraph 1 shall be any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial co-operation in criminal matters and police co-operation.

2a. The transferring competent authority shall inform the supervisory authority about transfers under this Article.

2b. When a transfer is based on paragraph 1, such a transfer must be documented.

*Article 37*

*(...)*

*Article 38*

***International co-operation for the protection of personal data***

1. In relation to third countries and international organisations, the Commission and Member States shall take appropriate steps to:

   (a) develop international co-operation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

   (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

   (c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

   (d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

2. (…)

## CHAPTER VI
## INDEPENDENT SUPERVISORY AUTHORITIES

### SECTION 1
### INDEPENDENT STATUS

*Article 39*

***Supervisory authority***

1. Each Member State shall provide that one or more independent public authorities are responsible for monitoring the application of this Directive, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union.

1a. Each supervisory authority shall contribute to the consistent application of this Directive throughout the Union. For this purpose, the supervisory authorities shall co-operate with each other and with the Commission in accordance with Chapter VII.

2. Member States may provide that a supervisory authority established under Regulation EU/XXX may be the supervisory authority referred to in this Directive and assumes responsibility for the tasks of the supervisory authority to be established under paragraph 1 of this Article.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which shall represent those authorities in the European Data Protection Board.

*Article 40*

***Independence***

1. Member States shall ensure that each supervisory authority acts with complete independence in performing the tasks and exercising the powers entrusted to it in accordance with this Directive.

2. Member States shall provide that the member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Directive, remain free from external influence, whether direct or indirect and neither seek nor take instructions from anybody.

3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. (…)

5. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, co-operation and participation in the European Data Protection Board.

6. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority.

7. Member States shall ensure that each supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that each supervisory authority has separate, public, annual budgets, which may be part of the overall state or national budget.

*Article 41*

***General conditions for the members of the supervisory authority***

1. Member States shall provide that each member of a supervisory authority must be appointed by means of a transparent procedure either: by the parliament; or the government; or the head of State of the Member State concerned; or by an independent body entrusted by Member State law with the appointment.

2. The member or members shall have the qualifications, experience and skills, notably in the area of protection of personal data, required to perform their duties and exercise their powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with the law of the Member State concerned.

4. A member may only be dismissed in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

5. (…)

*Article 42*

***Rules on the establishment of the supervisory authority***

1. Each Member State shall provide by law for:

   (a) the establishment of each supervisory authority;

   (b) the qualifications and eligibility conditions required to be appointed as a member of each supervisory authority;

   (c) the rules and procedures for the appointment of the members of each supervisory authority;

(d) the duration of the term of the member or members of each supervisory authority, which shall not be less than four years, except for the first appointment after entry into force of this Directive, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) whether and, if so, for how many terms the member or members of each supervisory authority shall be eligible for reappointment;

(f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

(g) (…)

1a The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, this duty of professional secrecy shall in particular apply to reporting by individuals of infringements of this Directive.

*Article 43*

*(…)*

## SECTION 2
## COMPETENCE, TASKS AND POWERS

*Article 44*

***Competence***

1. Member States shall provide that each supervisory authority shall be competent to perform the tasks and exercise the powers conferred on it in accordance with this Directive on the territory of its own Member State.

2. Member States shall provide that the supervisory authority is not competent to supervise processing operations of courts when acting in their judicial capacity. Member States may provide that the supervisory authority is not competent to supervise processing operations of other independent judicial authorities when acting in their judicial capacity.

*Article 45*

***Tasks***

1. Member States shall provide that each supervisory authority shall on its territory:

   (a) monitor and enforce the application of the provisions adopted pursuant to this Directive and its implementing measures;

   (aa) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data;

   (ab) advise, in accordance with national law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;

   (ac) promote the awareness of controllers and processors of their obligations under this Directive;

(ad) upon request, provide information to any data subject concerning the exercise of their rights under this Directive and, if appropriate, co-operate with the supervisory authorities in other Member States to this end;

(b) deal with complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 53, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(c) check the lawfulness of data processing pursuant to Article 15a, and inform the data subject within a reasonable period of the outcome of the check pursuant to Article 15a (2) or of the reasons why the check has not been carried out;

(d) cooperate with, including sharing information, and provide mutual assistance to other supervisory authorities, with a view to ensuring the consistency of application and enforcement of this Directive;

(e) conduct investigations on the application of this Directive, including on the basis of information received from another supervisory authority or other public authority;

(f) monitor relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

(g) (…)

(h) give advice on the processing operations referred to in Article 26;

(i) contribute to the activities of the European Data Protection Board.

2. (…)

3. (…)

4. Each supervisory authority shall facilitate the submission of complaints referred to in point (b) of paragraph 1, by measures such as providing a complaint submission form, which can be completed also electronically, without excluding other means of communication.

5. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and for the data protection officer.

6. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

*Article 46*

***Powers***

1. Each Member State shall provide by law that its supervisory authority shall have effective investigative powers, at least the power to obtain, from the controller and the processor, access to all personal data that is being processed and to all information necessary for the performance of its tasks.

   (a) (…)

   (b) (…)

   (c) (…)

(1a) Each Member State shall provide by law that its supervisory authority shall have effective corrective powers such as, for example:

   (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe the provisions adopted pursuant to this Directive;

(b) to order the controller or processor to bring processing operations into compliance with the provisions adopted pursuant to this Directive, where appropriate, in a specified manner and within a specified period; in particular by ordering the rectification, restriction or erasure of data pursuant to Article 15;

(c) to impose a temporary or definitive limitation, including a ban, on processing.

(1b) Each Member State shall provide by law that its supervisory authority shall have the effective advisory powers to advise the controller in accordance with the prior consultation procedure referred to in Article 26 and to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with national law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data.

2. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter of Fundamental Rights of the European Union.

3. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of provisions adopted pursuant to this Directive to the attention of judicial authorities and, where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions adopted pursuant to this Directive.

*Article 46a*

***Reporting of breaches***

Member States shall provide that the competent authorities shall put in place effective mechanisms to encourage confidential reporting of breaches of this Directive.

*Article 47*

***Activities report***

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of notified breaches and types of imposed sanctions. The report shall be transmitted to the national parliament, the government and other authorities as designated by national law. It shall be made available to the public, the Commission and the European Data Protection Board.

## CHAPTER VII
## CO-OPERATION

*Article 48*
***Mutual assistance***

1. Member States shall provide that supervisory authorities provides each other with relevant information and mutual assistance in order to implement and apply this Directive in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out consultations, inspections and investigations.

2. Member States shall provide that each supervisory authority takes all appropriate measures required to reply to the request of another supervisory authority without undue delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

2a. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

2b. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b) compliance with the request would be incompatible with the provisions of this Directive or with Union or Member State law to which the supervisory authority receiving the request is subject.

3. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to respond to the request. In cases of a refusal under paragraph 2b, it shall explain its reasons for refusing the request.

3a. Supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

3b. No fee shall be charged for any action taken following a request for mutual assistance. Supervisory authorities may agree with other supervisory authorities rules for indemnification by other supervisory authorities for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

3c. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).

*Article 49*

***Tasks of the European Data Protection Board***

1. The European Data Protection Board established by Regulation (EU)…./ XXX exercise the following tasks in relation to processing within the scope of this Directive:

(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Directive;

(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Directive and issue guidelines, recommendations and best practices in order to encourage consistent application of this Directive;

(ba) draw up guidelines for supervisory authorities concerning the application of measures referred to in paragraph 1 and 1b of Article 46;

(bb) issue guidelines, recommendations and best practices in accordance with point (b) for establishing the data breaches and determining the undue delay referred to in paragraphs 1 and 2 of Article 28 and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(bc) issue guidelines, recommendations and best practices in accordance with point (b) as to the circumstances in which a personal data breach is likely to result in a high risk for the rights and freedoms of the individuals referred to in Article 29 (1);

(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and (ba);

(d) give the Commission an opinion for the assessment of the adequacy of the level of protection in a third country or international organization, including for the assessment whether a third country or the territory or the international organization or the specified sector no longer ensures an adequate level of protection. To that end, the Commission shall provide the European Data Protection Board with all necessary documentation, including correspondence with the government of the third country, territory or processing sector within that third country or the international organisation.

(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;

(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;

(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

2. Where the Commission requests advice from the European Data Protection Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 57(1) and make them public.

4. The Commission shall inform the European Data Protection Board of the action it has taken following opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.

## CHAPTER VIII
## REMEDIES, LIABILITY AND SANCTIONS

*Article 50*

***Right to lodge a complaint with a supervisory authority***

1. Without prejudice to any other administrative or judicial remedy, Member States shall provide that every data subject shall have the right to lodge a complaint with a single supervisory authority, if the data subject considers that the processing of personal data relating to him or her does not comply with provisions adopted pursuant to this Directive.

1a. Member States shall provide that if the complaint is not lodged with the supervisory authority that is competent pursuant to Article 44 (1), the supervisory authority with which the complaint has been lodged shall transmit it to the competent supervisory authority, without undue delay. The data subject shall be informed about the transmission.

1b. Member States shall provide that the supervisory authority with which the complaint has been lodged provides further assistance upon request of the data subject.

2. (…)

2a. The data subject shall be informed by the competent supervisory authority of the progress and the outcome of the complaint, including of the possibility of a judicial remedy pursuant to Article 51.

3. (…)

*Article 51*

***Right to an effective judicial remedy against a supervisory authority***

1. Without prejudice to any other administrative or non-judicial remedy, Member States shall provide for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority competent in accordance with Article 44 (1) does not deal with a complaint or does not inform the data subject within three months of the progress or outcome of the complaint lodged under Article 50.

3. Member States shall provide that proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

*Article 52*

***Right to a judicial remedy against a controller or processor***

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority under Article 50, Member States shall provide for the right of data subjects to an effective judicial remedy if they consider that their rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of their personal data in non-compliance with these provisions.

*Article 53*

***Representation of data subjects***

1. Member States shall, in accordance with national procedural law, provide that the data subject shall have the right to mandate a body, organisation or association, which has been properly constituted according to the law of a Member State, which is of non-profit making character, and whose statutory objectives are in the public interest and which is active in the field of protection of data subject's rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf and to exercise the rights referred to in Articles 50, 51 and 52 on his or her behalf.

2. (…)

3. (…)

*Article 54*

***Right to compensation***

1. Member States shall provide that any person who has suffered material or immaterial damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive shall have the right to receive compensation for the damage suffered from the controller or any other authority competent under national law.

2. (…)

3. (…)

*Article 55*

***Penalties***

Member States shall lay down the rules on penalties, applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive.

## CHAPTER IX
## IMPLEMENTING ACTS

*Article 56*

*(…)*

*Article 57*

***Committee procedure***

1. The Commission shall be assisted by the committee established by Article 87 of Regulation (EU) XXX. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

## CHAPTER X
## FINAL PROVISIONS

*Article 58*

***Repeals***

1. Council Framework Decision 2008/977/JHA is repealed with effect from the date referred to in Article 62(1).

2. References to the repealed Framework Decision referred to in paragraph 1 shall be construed as references to this Directive.

*Article 59*

***Relationship with previously adopted acts of the Union for judicial co-operation in criminal matters and police co-operation***

The specific provisions for the protection of personal data in acts of the Union adopted in the field of judicial co-operation in criminal matters and police co-operation adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive remain unaffected.

*Article 60*

***Relationship with previously concluded international agreements in the field of judicial co-operation in criminal matters and police co-operation***

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to the entry into force of this Directive, and which are in compliance with Union law, applicable prior to the entry into force of this Directive, shall remain in force until amended, replaced or revoked.

*Article 61*

***Evaluation***

1. The Commission shall submit reports on the evaluation and review of this Directive to the European Parliament and the Council at regular intervals.

1a. In the context of these evaluations and reviews, the Commission shall examine, in particular, the application and functioning of the provisions of Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Articles 34, paragraph 3 and 36aa.

1b. For the purposes referred to in paragraphs 1 and 1a, the Commission may request information from Member States and supervisory authorities.

1c. In carrying out the evaluations and reviews referred to in paragraphs 1 and 1a, the Commission shall take into account the positions and findings of the European Parliament, the Council as well as other relevant bodies or sources.

1d. The first reports shall be submitted no later than four years after the date of implementation of this Directive. Subsequent reports shall be submitted every four years thereafter. The reports shall be made public.

1e. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Directive and aligning other legal instruments, in particular taking account of developments in information technology and in the light of the state of progress in the information society.

2. The Commission shall review within three years after the entry into force of this Directive other acts adopted by the European Union which regulate the processing of personal data by the competent authorities for the purposes set out in Article 1(1) including those acts adopted by the Union referred to in Article 59, in order to assess the need to align them with this Directive and make, where appropriate, the necessary proposals to amend these acts to ensure a consistent approach on the protection of personal data within the scope of this Directive.

3. (…)

*Article 62*

***Implementation***

1. Member States shall adopt and publish, by [date/two years after the entry into force]at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions. They shall apply those provisions from xx.xx.201x [date/two years after the entry into force].

   When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

1a. By way of derogation from paragraph 1, Member States may provide that, exceptionally, where it involves disproportionate effort, the automated processing systems set up before the date of entry into force of this Directive shall be brought into conformity with Article 24 (1) within 7 years of the date of entry into force of this Directive.

1b. In exceptional circumstances, a Member State may bring a particular automated processing system set up before the date of entry into force of this Directive into conformity with Article 24(1) within a specified period after the period referred to in paragraph 1a, if it would otherwise cause serious difficulties for the operation of that particular automated processing system. It shall notify the Commission of the grounds for these serious difficulties and the grounds for the specified period within which it shall bring that particular automated processing system into conformity with Article 24(1). The specified period shall in any event not exceed three years after the period referred to in paragraph 1a.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

*Article 63*

***Entry into force***

This Directive shall enter into force on the first day following that of its publication in the Official Journal of the European Union.

*Article 64*

***Addressees***

This Directive is addressed to the Member States.

Done at …,

| | |
|---|---|
| *For the European Parliament* | *For the Council* |
| *The President* | *The President* |